

CONTRACT #2020-DD-24

between

CLARK COUNTY

P.O. Box 5000, Vancouver, WA 98666-5000

and

EDUCATIONAL SERVICE DISTRICT #1122500 NE 65th Avenue, Vancouver, WA 98661-6812**Program:****Child Development Services**

Contract Period:

July 1, 2019 through June 30, 2020

Contract Amount:

\$102,854.40

Funding Sources:

Fund 1953 State DDA and DD Property Tax

DUNS Number:

091293175

CFDA Number:

None

CONTRACTOR CONTACT	COUNTY CONTACT
Carol Hall 360.952.3514 carol.hall@esd112.org	Kristin Wade 564.397.7830 kristin.wade@clark.wa.gov

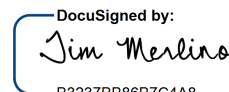
By signing below, Clark County, hereinafter referred to as the "County," and Educational Service District #112, hereinafter referred to as the "Contractor," agree to the terms of this Contract as well as the Clark County Community Services General Terms and Conditions, as amended, which are incorporated herein by reference with the same force and effect as if they were incorporated in full text. The full text version of the County's General Terms and Conditions are available at <https://www.clark.wa.gov/community-services/general-terms-and-conditions>. Hard copies will be provided by Clark County upon request.

FOR CLARK COUNTY:

DocuSigned by:

7/12/2019
020976145587476
Shawn Hennessee, County Manager

FOR EDUCATIONAL SERVICE DISTRICT #112:

DocuSigned by:

7/8/2019
B3237BB86B7C4A8
Tim Merlino, Chief Executive Officer

APPROVED AS TO FORM ONLY:

DocuSigned by:

7/8/2019
F6B2CB11526542F...
Amanda Migchelbrink
Deputy Prosecuting Attorney

BUDGET SUMMARY
CONTRACT 2020-DD-24
EDUCATIONAL SERVICE DISTRICT #112

Fund	Grant	Cost Center	Basubs	Program	Program Description	Payment Type	Activity	Spending Category	Amount
9017 (1953)	GR0000024	CC202 DD	B5680000	PG0160	Child Development Services	Fee-For-Service	Varies	S0081 Professional Services	\$102,854.40
1953	N/A				All approved program lines				\$0
								Total	\$102,854.40

**STATEMENT OF WORK #1
CONTRACT 2020-DD-24
EDUCATIONAL SERVICE DISTRICT #112**

1. SERVICE DESCRIPTION

The goal of Child Development Services is to enhance the development of infants and toddlers with disabilities and to minimize their developmental delays. Child Development Services are designed to meet the developmental needs of each eligible child and the needs of the family related to enhancing the child's development. Services may include specialized instruction, speech-language pathology, occupational therapy, physical therapy, assistive technology, and vision services. Services are provided in natural environments and intended to promote improved positive social-emotional skills (including social relationships); acquisition and use of knowledge and skills (including early language/communication); and use of appropriate behaviors to meet their needs. Services shall be designed to match the preferences, hopes and strengths of the family and enhance their capacity to meet the special needs of their infants and toddlers with disabilities.

2. CONTRACTOR REQUIREMENTS

The Contractor shall ensure that the training, experience, and expertise of their staff meet the highest entry-level requirements in Washington State for Early Intervention Professionals and relate to the needs of the participants, as outlined in Developmental Disabilities Administration (DDA) Policy 6.13.

The Contractor shall provide to the County Developmental Disabilities Program Coordinator a schedule of business hours for each calendar year within fifteen (15) days of the beginning of the contract. The schedule shall include regular days and hours of operations, observed holidays and planned closures.

3. AUTHORIZED EARLY INTERVENTION SERVICES

The Contractor shall provide one (1) or more of the Early Intervention Services listed below, as defined by Washington State's Federally Approved Plan for the Early Support for Infants and Toddlers Program Department of Early Learning Under the Individuals with Disabilities Education Act (IDEA) Early Intervention Section

Only services provided in natural environments are funded in this Statement of Work.

- 3.1. Family training, counseling, and home visits
- 3.2. Occupational therapy
- 3.3. Physical therapy
- 3.4. Specialized instruction
- 3.5. Speech/Language Pathology

4. PROGRAM REQUIREMENTS

It is expected that services will be delivered within a multi-disciplinary team and using a primary coach approach. One (1) member of a multi-disciplinary team will be assigned as the principal coach and point of contact for the child and family. The primary coach is responsible for the child/family outcomes as identified on the child's Individual Family Service Plan (IFSP). Other therapists and/or educators provide support to the primary coach and may provide services to the child as needed to meet the outcomes identified on the IFSP.

The Contractor shall provide services as outlined below:

- 4.1. Evaluation (eligibility), assessment (child and family need) and the Individualized Family Service Plan (IFSP) shall be conducted within 45 days of receipt of referral. (Referral is defined as the date the family has been informed of the opportunity for services, of their rights, and they indicate a desire to pursue services).
- 4.2. Collaborate with the child's Family Resources Coordinator in the development of an Individual Family Service Plan (IFSP).
 - 4.2.1. Child and family outcomes within the IFSP are functional and based on the individualized needs of the infant or toddler and the concerns and the priorities of the family.
 - 4.2.1.1. Child specific outcomes reflect the child's participation in everyday routines and activities.
 - 4.2.1.2. Family specific outcomes address the capacity of the family to enhance their child's development.
 - 4.2.2. Services consistent with the IFSP will be started within thirty (30) days of the start date on the signed IFSP unless the IFSP documents that the parent requested a delay in the start of the service(s).
 - 4.2.3. Participate in the IFSP review at a minimum of every six (6) months, or more frequently if conditions warrant, and write a new IFSP annually. Service changes indicated by this review will be initiated at the time of the review.
 - 4.2.4. Progress toward the child and family outcomes within the IFSP are assessed on an ongoing basis and documented at least annually.
- 4.3. Contractor shall obtain from the parent, in writing, consent for all activities related to the provision of early intervention service in the family's native language or other mode of communication.
- 4.4. Services must be provided in the most natural environment for each child including in-home services. Natural environments are settings that are natural or normal for the child's age peers who have no disabilities (*US Code of Federal Regulations 303.18*). These services are provided in the home, neighborhood, or community settings in which children without disabilities participate (*Washington State's Application for Federal*

Funds, Section III-12).

- 4.4.1 Community-Based Service Definition: Services provided in a setting where children without disabilities typically are found. These settings include but are not limited to: child care centers (including family day care), preschools, regular nursery schools, libraries, grocery stores, parks, restaurants, and community centers (e.g. YMCA, Boys and Girls Clubs). Services provided in a hospital, residential facility, clinic, and Early Intervention center/class designed for children with disabilities are not considered community-based.
- 4.5. Support the continued development of this service through activities such as, but not limited to, reviewing draft documents and providing feedback to the County, participating in all County required trainings and attending all service development meetings.
- 4.6. Document that each family is assisted to ensure the child obtains an evaluation by a multidisciplinary team and that the evaluation used to determine eligibility shall:
 - 4.6.1. Be completed in accordance with the Early Support for Infants and Toddlers Practice Guide: Evaluation, Assessment, Eligibility and the Initial IFSP <https://www.dcyf.wa.gov/sites/default/files/pdf/esit/EvaluationAssessmentSept2013.pdf>
 - 4.6.2. Document that the child demonstrates a delay of 1.5 standard deviation or 25% of chronological age delay in one (1) or more of the developmental areas.
 - 4.6.3. Include the name and discipline of the clinician performing the evaluation shall be included on all evaluation reports.
 - 4.6.4. Be conducted within forty-five (45) days of receipt of referral. (Referral is defined as the date the family has been informed of the opportunity for services, of their rights, and they indicate a desire to pursue services).
- 4.7. Participate in the development of a transition plan, for each child, ninety (90) days prior to the child's third birthday, in collaboration with the local school district and the local lead agency.
- 4.8. Participate in the development of a complete a Child Outcome Summary (COS), for each child, at the beginning and end of the child's services.
- 4.9. Provide services in a manner that supports the cultural and ethnic diversity of families.
- 4.10. Ensure that eligible families have access to interpreter services when needed to effectively participate in Child Development Services.
5. The Contractor will comply with established guidelines, requirements, and criteria for service documentation:

- 5.1. The Contractor shall email to the County Contact person, the number County approved children that the Contractor provided services to in a natural environment. The Contractor shall include all children that have a County approval for each month, even if the services were not billed to the County. The Contractor shall submit these quarterly numbers with their CMIS billing for the following service months: September, December, March and June of each calendar year.

6. PAYMENT

In addition to the contract terms listed in the Clark County Community Services General Terms and Conditions, the following shall apply:

- 6.1. Services will be paid as a monthly case rate for a minimum of 1 hour of service provided to each eligible customer. **The monthly case rate is \$214.28.**
- 6.2. The County will pay only for Early Intervention activities provided individually and in natural environments. This funding is intended to augment other funding sources available to the Contractor in providing services to eligible customers.
- 6.3. The Contractor shall not exceed the annual allocation of children to be served.
- 6.4. Services shall be provided in accordance with County Policy DCS 31 – Service Definitions and Coding and the County authorization of services.
- 6.5. The County may request that the Contractor purchase equipment or other special program-specific items for the effective provision of services to individuals with developmental disabilities. The County will reimburse the Contractor for these required items subject to prior written approval by the County. The approval shall be based upon written documentation submitted by the Contractor to include vendor name, cost, product model, and a thorough description of the requested item(s).
- 6.6. The Contractor shall bill for services in accordance with the Payment and Billing Provisions and Reporting Requirements Section in the Special Terms and Conditions of this Contract and criteria referenced in this Statement of Work.
- 6.7. The Contractor shall invoice the County no later than the 10th of the month following each month of service. Invoices shall identify the month and year of service, the Contract number, and all services being billed for the previous month. Services billed more than sixty (60) days after the date of service will not be paid as the County will not be able to bill the State.
 - 6.7.1. The Contractor shall submit a CMIS Report with each invoice that includes all customers authorized by the County for service without regard to source of funding.
 - 6.7.2. If requested by the County, the Contractor shall report all funds received for customers who have multiple funding sources for any service provided under this Contract.

- 6.8. The Contractor shall bill only for services to customers who:
 - 6.8.1. Are authorized for service through a County Approval
 - 6.8.2. Have a Service Plan
 - 6.8.3. Are accepted for service by the Contractor
- 6.9. Reporting erroneous service information regarding a County-funded customer may result in corrective action, may constitute Medicaid fraud or abuse, and possible result in contract termination.
- 6.10. Overbilling the County for any reason may result in corrective action, repayment, and may result in Contract termination. All such actions will be reviewed for evidence of fraud or abuse.
- 6.11. Funds received from the County shall not be used to provide cash benefit to the supported customer or family member, whether salary, bonuses, or benefits.
- 6.12. The number of eligible children to be funded under this Statement of Work is reviewed by the County at least annually based on consumer choice of service providers and the total number of County-funded children.

SPECIAL TERMS AND CONDITIONS DEVELOPMENTAL DISABILITIES PROGRAM

JULY 2019

Child Development Services

1. DOCUMENTS INCORPORATED BY REFERENCE

Each of the documents listed below, as now established or hereafter amended, are incorporated by reference with the same force and effect as if they were incorporated in full text.

- 1.1. The DSHS and County Agreement on General Terms and Conditions available at:
<https://www.dshs.wa.gov/dda/county-best-practices>
- 1.2. The County Program Agreement with DSHS for DDA County Services and subsequent agreements and amendments
- 1.3. DSHS DDA Policies, available at:
<https://www.dshs.wa.gov/dda/policies-and-rules/policy-manual>
- 1.4. Clark County Developmental Disabilities Program Policies and Procedures
- 1.5. Home and Community-Based Services Waiver (0408) in Accordance with Section 1915(C) of the Social Security Act
- 1.6. The Budgeting and Accounting Reporting System (BARS)
- 1.7. Washington Protection and Advocacy Access Agreement, available at:
<https://www.dshs.wa.gov/sites/default/files/DDA/dda/documents/WPAS.pdf>
- 1.8. DDA Criteria for Evaluation available at:
<https://www.dshs.wa.gov/dda/county-best-practices>
- 1.9. WAC 388-850, WAC 388-845, WAC 388-828
- 1.10. County Guide to Achieve DDA Guiding Values
<https://www.dshs.wa.gov/sites/default/files/DDA/dda/documents/County%20Guide%20Guiding%20Values%202018.docx>
- 1.11. Clark County Department of Community Services General Terms and Conditions.
- 1.12. Contractor Travel Reimbursement Policy attached as Exhibit A
- 1.13. Business Associate Agreement attached as Exhibit B
- 1.14. Data Security Requirements attached as Exhibit C

2. DRUG-FREE WORKPLACE POLICY

The Contractor shall have a “Drug-Free Workplace” Policy that describes the steps taken to deter the use of drugs, including alcohol, in the workplace and that addresses the Drug-Free Workplace Act of 1988. The policy should include any provisions for education, scope of prohibited substances, testing, employee assistance, discipline, and employee responsibilities.

3. ELIGIBILITY FOR SERVICES

Only customers determined eligible by DDA and/or approved for funding by the County shall be eligible for services reimbursed under this Contract. Funding must be approved by the County prior to the provision of any services under this agreement.

4. INSURANCE

In addition to the contract terms listed in the Clark County Department of Community Services General Terms and Conditions, the Contractor shall not be required to provide fidelity and professional liability insurance.

5. LIMITED ENGLISH PROFICIENCY

In addition to the contract terms listed in the Clark County Department of Community Services General Terms and Conditions, the Contractor shall ensure that all employees review DDA Policy 5.05 and that all customers receive accommodations in compliance with Limited English Proficiency policies.

6. OPERATIONAL REQUIREMENTS

The Contractor shall adhere to the following procedures in providing services and business operations:

- 6.1. Ensure that all staff members receive required training as determined by DDA Policy 6.13 Provider Qualifications for Employment and Day Program Services and the Clark County DD Program that meets County and State approved standards and the needs of customers in service. All staff members shall receive required trainings every two (2) years after initial training. Proof of trainings shall be kept in personnel files. All training requirements are the responsibility of the Contractor and shall include training indicated in DDA Policy 6.13 and the following:

- 6.1.1. Washington Protection and Advocacy Access Agreement

- 6.1.2. County Guide to Achieve DDA Guiding Values
<https://www.dshs.wa.gov/sites/default/files/DDA/dda/documents/County%20Guide%20Guiding%20Values%202018.docx> (sections as applicable to children and youth)

- 6.2. The Contractor shall communicate directly with the assigned County Program

Coordinator on issues related to service provision and/or funding for supported customers. All required submissions regarding this Contract shall also be directed to the assigned County Program Coordinator, including communication regarding planning, exceptions to policy, and incidents.

The Contractor shall return all phone calls and emails within two (2) business days.

6.3. The Contractor shall follow these procedures regarding customers' health and safety:

- 6.3.1. Adhere to DDA Policy 6.08: Incident Management and Reporting Requirements for County and County Contracted Providers. The Contractor's staff members are considered "mandated reporters" under RCW 74.34.020(11) and must comply with reporting requirements described in RCW 74.34.035.040 and Chapter 26.44 RCW and the County DD Program requirements regarding incident reporting.

If the Contractor is notified by the County or DSHS that a staff member has been cited or is on the registry for a substantiated finding, then that staff member must be prohibited from providing services under this Contract.

- 6.3.2. Complete notification and a written incident report within the timeframes indicated in DDA Policy 6.08 and submit to Clark County, DDA case management, other agencies as appropriate. The report shall be filed on a County Incident Reporting form.

- 6.3.3. Ensure that emergency contact and medical information (medications, diet, allergies, etc.) needed during the hours of service is available for each customer.

- 6.3.4. Employ staff aged 18 years or older and conduct a background criminal history clearance every three (3) years for all employees, subcontractors, and/or volunteers who may have unsupervised access to vulnerable DSHS customers, in accordance with RCW 43.43.830-845, RCW 74.15.030, WAC Chapter 388.06, and 388-825. The DSHS Background Check Central Unit (BCCU) shall be utilized to obtain all background clearances.

If the Contractor elects to hire or retain an individual after receiving notice that the applicant has a conviction for an offense that would automatically disqualify the applicant from having unsupervised access to children and/or vulnerable adults as defined in RCW Chapter 74.34.020 Definitions, the County shall deny payment for any subsequent services rendered by the disqualified staff.

- 6.3.5. The Contractor shall ensure all services are provided in accordance with the DDA Criteria for Evaluation, federal, state and local safety standards.

- 6.3.6. For Child Development service providers, the Contractor's employees must have a valid Washington State credential prior to employment if the position requires the employee to be registered, certified, or licensed under Washington State law for the service(s) the Contractor intends to provide under Contract.

- 6.4. Maintain and adhere to a County-approved written grievance procedure for customers in accordance with the DDA Criteria for Evaluation and DDA Necessary Supplemental Accommodation (NSA) Policy 5.02 and that it:
 - 6.4.1. Is explained to the customer and, if necessary, to a family member, guardian or advocate
 - 6.4.2. Provides for negotiation of conflicts
 - 6.4.3. Provides a mediation process using someone who is unaffected by the outcome if conflicts remain unresolved and may include the DDA Case Manager as an alternative option
 - 6.4.4. Promotes the availability of and encourages the use of advocates by customers to help negotiate conflicts
 - 6.4.5. Prohibits retaliation for using the grievance process
 - 6.4.6. Includes a process for tracking and reporting grievances
 - 6.4.7. Acknowledges that all customers have freedom of choice of providers and shall cooperate with the County and DDA to ensure this right. This includes directing customers to their DDA Case Managers if they indicate an interest in changing services or providers
 - 6.4.8. Has timelines for filing and responses
 - 6.4.9. Has formal and informal process for resolution, including arbitration, if necessary
 - 6.4.10. Notifies the County and DDA Case Manager when a grievance requires formal arbitration
 - 6.4.11. Notifies the customer that they may contact the County and DDA Case Manager if unsatisfied with Contractor response
 - 6.4.12. Documents the customer's receipt of written procedure in the customer's file
- 6.5. The Contractor shall cooperate and collaborate with the County, other entities, the customer and family members in the provision of services, planning and information sharing, and meet with the County upon request.
- 6.6. The Contractor, the Contractor's Board Members, or the Contractor's staff shall not serve as an employer or a decision-maker for a customer or a customer's family members or provide any form of guardianship, legal representation, payee, or residential supports to customers receiving services under this Contract. This provision may be waived upon written approval of the County.
- 6.7. Prior to releasing any confidential information, the Contractor will secure Release of

Information (ROI) forms that, at a minimum:

- 6.7.1. Include the name, address, phone number and contact person of the entity requesting the information
- 6.7.2. Identify only one (1) entity to receive the request for information, with that entity clearly identified
- 6.7.3. State specific information being requested and the purpose for the request
- 6.7.4. Prohibit the re-release of information
- 6.7.5. Include an expiration date for the request. The expiration date may not be more than ninety (90) days from the date of the request. In some instances where there is a need for on-going communication, such as DVR or a County service provider, the release may be for a maximum of one (1) year and must indicate the end date
- 6.7.6. Include the customer's or legal guardian's signature and date of signature
- 6.8. The Contractor shall have a written performance plan that describes program objectives, expected outcomes, how and when objectives and outcomes will be accomplished, and shall have an administrative/organizational structure that clearly defines responsibilities, including a current organizational chart and job descriptions. The plan shall be evaluated at least biennially and revised based on actual performance.

The Contractor shall submit a copy of their written performance plan to the County for approval within 60 days of contract execution.

The Contractor shall develop and maintain sufficient policies and procedures for establishment and maintenance of adequate internal control systems: The Contractor will maintain written policy procedural manuals for information systems, personnel, and accounting/finance in sufficient detail such that operations can continue should staffing change or absences occur.
- 6.9. Each individual shall have one (1) file with a table of contents. All service documentation shall be included in the file. In the event that the file becomes full, a Volume II shall be created for the customer. An individual case note shall be created for each individual and shall correlate with each individual's service billed to the County. All case notes shall be in chronological order. Older case notes will be in the back and the most recent case notes will be in the front. Other forms of documentation will not be accepted when reviewing files for billing verification.

Minimum standards for case notes:

- 6.9.1. Customer name
- 6.9.2. Date of service
- 6.9.3. Start time

- 6.9.4. Duration of services (in minutes)
- 6.9.5. Description of services provided
- 6.9.6. Service setting
- 6.9.7. Authentication, including printed name, and title of person providing service

7. TERMINATION

- 7.1. The award or continuation of this Contract is dependent upon the availability of future funding. The County's payment obligations are payable only and solely from funds both appropriated and otherwise legally available for this Contract.
 - 7.1.1. The absence of initial appropriated or other lawfully-available funds shall render the Contract null and void to the extent funds are not appropriated or available.
 - 7.1.2. If the funds upon which the County relied to establish this Contract are withdrawn, reduced, or limited, or if additional or modified conditions are placed on such funding, the County may immediately terminate this Contract in whole or in part by providing notice to the Contractor. The termination shall be effective on the date specified in the notice of termination.
- 7.2. The County shall have the right to terminate this Contract, in whole or in part, with or without cause, by providing no fewer than ten (10) calendar-days written notice. Upon receipt of a notice of termination, the Contractor shall promptly cease all further work pursuant to this Contract, with such exceptions, if any, specified in the notice of termination. The County shall pay the Contractor, to the extent of funds appropriated or otherwise legally available for such purpose, for all goods delivered, services performed, and obligations incurred prior to the date of termination in accordance with the terms hereof.
- 7.3. Upon termination of this Contract any unexpended balance of Contract funds will remain with the County. If termination occurs for cause, the Contractor shall immediately, and without notice of presentment, return to the County all funds that were expended in violation of the terms of this Contract.
- 7.4. Any notice required to be given pursuant to the terms of this section shall be in writing and shall be sent by certified or registered mail, return receipt requested, postage prepaid, or by hand delivery, to the receiving party at the address listed on the signature page, or at any other address of which a party has given notice. Notice shall be deemed given on the date of delivery or refusal as shown on the return receipt if delivered by mail, or the date upon which such notice is personally delivered in writing.

8. WRITTEN CORRESPONDENCE

Contractor shall mail correspondence associated with this Statement of Work to the attention of the County Contact at the following address:

Clark County
Department of Community Services
Attn: County Contact
P.O. Box 5000
Vancouver, WA 98666

EXHIBIT A**CONTRACTOR TRAVEL REIMBURSEMENT POLICY**

For contracts which allow travel reimbursements, the Contractor shall comply with the Clark County Travel Policy. The following travel related expenses are allowable if incurred in conjunction with travel for the performance of work under contract with Clark County.

- **Local travel expenses:** those incurred within a 50 mile radius of the Contractor's business location and/or travel more than 50 miles that does NOT include an overnight stay
 - Mileage
 - Parking
 - Business meals at actual cost. Total, including tax and tips, should not exceed the current IRS High-Low per diem rate
- **Non-local travel expense:** those incurred more than 50 miles from the Contractor's business location and include an overnight stay
 - Airfare, bus, train, local transportation, tolls, car rentals and parking fees.
 - Mileage - In instances where personal automobile usage exceeds the cost of airfare, reimbursement will be limited to the cost of traveling to the same destination by coach class airfare.
 - Hotel or motel accommodations at single occupancy rates. The lowest rate should be requested.
 - Meal costs at the per diem rates established by the Internal Revenue Service using the High-Low substantiation method. Employees will be allowed 75% of the daily per diem allowance on the first and last day of travel and 100% of the daily per diem allowance the remainder of the trip.
 - Other reasonable and ordinary expenses which are job related and incurred while representing the county on official business.

Itemized receipts must be provided for meals at actual cost, lodging, and all other travel related expenses. If the travel expense involves a conference, workshop, seminar, or similar organized activity, a copy of the agenda or outline must be submitted.

The current per diem rates and mileage rates can be located at <https://www.clark.wa.gov/community-services/travel>.

2019	Low	High
Breakfast	12	17
Lunch	18	22
Dinner	30	32

EXHIBIT B**BUSINESS ASSOCIATE AGREEMENT**

This Business Associate Agreement (BAA) and Qualified Service Organization Agreement (QSOA) is entered into between Clark County Department of Community Services (the “Covered Entity”) and Educational Service District 112 (the “Business Associate”).

Recitals

- A. Business Associate provides **Child Development Services** for Covered Entity (the “Services”) which sometimes may involve (i) the use or disclosure of Protected Health Information (as defined below) by Business Associate, (ii) the disclosure of Protected Health Information by Covered Entity (or another business associate of Covered Entity) to Business Associate, or (iii) the creation, receipt, maintenance, or transmission of Electronic Protected Health Information (as defined below) by Business Associate. Accordingly, the use, disclosure, transmission, or maintenance of Protected Health Information by Business Associate is subject to the privacy regulations (the “HIPAA Privacy Regulations”) and the security regulations (the “HIPAA Security Regulations”) promulgated pursuant to the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”), and 45 C.F.R. Parts 160 and 164 with respect to such Services. This Agreement is intended to document the business associate assurances required by the HIPAA Privacy Regulations (at 45 C.F.R. § 164.504(e)), and the HIPAA Security Regulations (at 45 C.F.R. § 164.314(a)).
- B. This Agreement will govern the terms and conditions under which Covered Entity may disclose or have disclosed to Business Associate, and Business Associate may create, use, disclose, maintain, transmit or receive, Protected Health Information on behalf of Covered Entity. This Agreement will also govern the terms and conditions under which Covered Entity may disclose or have disclosed to Business Associate, and Business Associate may create, receive, maintain or transmit, EPHI on behalf of Covered Entity.

Agreement

1. Definitions. Capitalized terms used in this Agreement, but not otherwise defined in this Agreement, shall have the same meanings as those terms in the HIPAA Privacy Regulations and the HIPAA Security Regulations. Unless otherwise stated, a reference to a “Section” is to a Section in this Agreement. For purposes of this Agreement, the following terms shall have the following meanings.
 - 1.1. Breach. “Breach” shall have the same meaning as the term “breach” in 45 C.F.R. § 164.402.
 - 1.2. Designated Record Set. “Designated Record Set” shall have the same meaning as the term “designated record set” in 45 C.F.R. § 164.501.
 - 1.3. Electronic Protected Health Information or EPHI. “Electronic Protected Health Information” or “EPHI” shall have the same meaning as the term “electronic protected health information” in 45 C.F.R. § 160.103, limited to the information created or received by Business Associate from or on behalf of Covered Entity.

- 1.4. Individual. “Individual” shall mean the person who is the subject of Protected Health Information as provided in 45 C.F.R. § 160.103 and shall include a person who qualifies as a personal representative in accordance with 45 C.F.R. § 164.502(g).
 - 1.5. Individually Identifiable Health Information. “Individually Identifiable Health Information” shall have the same meaning as the term “individually identifiable health information” in 45 C.F.R. § 160.103.
 - 1.6. Protected Health Information or PHI. “Protected Health Information” or “PHI” shall have the same meaning as the term “protected health information” in 45 C.F.R. § 160.103, limited to the information created or received by Business Associate from or on behalf of Covered Entity.
 - 1.7. Required By Law. “Required By Law” shall have the same meaning as the term “required by law” in 45 C.F.R. § 164.103.
 - 1.8. Secretary. “Secretary” shall mean the Secretary of the federal Department of Health and Human Services or that person’s designee.
 - 1.9. Security Incident. “Security Incident” shall have the same meaning as the term “security incident” in 45 C.F.R. § 164.304.
 - 1.10. Unsecured Protected Health Information. “Unsecured Protected Health Information” shall have the same meaning as the term “unsecured protected health information” in 45 C.F.R. § 164.402, limited to the information created or received by Business Associate from or on behalf of Covered Entity.
2. Permitted Uses and Disclosures by Business Associate.
- 2.1. General. Except as otherwise specified in this Agreement, Business Associate may use or disclose PHI to perform its obligations for, or on behalf of, Covered Entity, provided that such use or disclosure would not violate the HIPAA Privacy Regulations if done by Covered Entity or the minimum necessary policies and procedures of Covered Entity.
 - 2.2. Other Permitted Uses. Except as otherwise limited by this Agreement, Business Associate may use PHI it receives or creates in its capacity as a business associate of Covered Entity, if necessary:
 - 2.2.1. For the proper management and administration of Business Associate;
 - 2.2.2. To carry out the legal responsibilities of Business Associate; or
 - 2.2.3. To provide Data Aggregation services to Covered Entity which relate to the health care operations of Covered Entity in accordance with the HIPAA Privacy Regulations.
 - 2.3. Other Permitted Disclosures. Except as otherwise limited by this Agreement, Business Associate may disclose to a third party PHI it receives or creates in its capacity as a business associate of Covered Entity for the proper management and administration of Business Associate, provided that:

2.3.1. The disclosure is Required by Law; or

2.3.2. Business Associate obtains reasonable assurances from the third party to whom the information is disclosed that (i) the PHI will remain confidential and used or further disclosed only as Required By Law or for the purpose for which it was disclosed to the third party, and (ii) the third party notifies Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

2.4. De-Identified Information. Health information that has been de-identified in accordance with the requirements of 45 C.F.R. §§ 164.514 and 164.502(d) and is therefore not Individually Identifiable Health Information (“De-Identified Information”) is not subject to the provisions of this Agreement. Covered Entity may disclose PHI to Business Associate to use for the purpose of creating De-Identified Information, whether or not the De-Identified Information is to be used by Covered Entity.

3. Obligations and Activities of Business Associate Regarding PHI.

3.1. Limitations on Uses and Disclosures. Business Associate will not use or further disclose PHI other than as permitted or required by this Agreement or as Required By Law.

3.2. Safeguards. Business Associate will use appropriate safeguards to prevent use or disclosure of the PHI other than as provided for by this Agreement.

3.3. Mitigation. Business Associate will mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of PHI by Business Associate in violation of the requirements of this Agreement.

3.4. Reporting. Business Associate will report to Covered Entity any use or disclosure of the PHI not provided for by this Agreement of which it becomes aware.

3.5. Agents and Subcontractors. Business Associate will ensure that any agent, including any subcontractor, to whom Business Associate provides PHI received from, or created or received by Business Associate on behalf of, Covered Entity agrees to the same restrictions and conditions that apply through this Agreement to Business Associate with respect to such information.

3.6. Access. Where PHI held by Business Associate is contained in a Designated Record Set, within fifteen (15) days of receiving a written request from Covered Entity, Business Associate will make such PHI available to Covered Entity or, as directed by Covered Entity to an Individual, that is necessary for Covered Entity to respond to Individuals’ requests for access to PHI about them in accordance with 45 C.F.R. § 164.524. Business Associate will provide such PHI in an electronic format upon request by Covered Entity unless it is not readily producible in such format in which case Business Associate will provide Covered Entity a standard hard copy format.

3.7. Amendment of PHI. Where PHI held by Business Associate is contained in a Designated Record Set, within fifteen (15) days of receiving a written request from Covered Entity or an Individual, Business Associate will make any requested

amendment(s) or correction(s) to PHI in accordance with 45 C.F.R. § 164.526.

- 3.8. Disclosure Documentation. Business Associate will document its disclosures of PHI and information related to such disclosures as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 C.F.R. § 164.528.
- 3.9. Accounting of Disclosures. Within thirty (30) days of receiving a request from Covered Entity, Business Associate will provide to Covered Entity information collected in accordance with Section 3.8 of this Agreement, as necessary to permit Covered Entity to make an accounting of disclosures of PHI about an Individual in accordance with 45 C.F.R. § 164.528.
- 3.10. Access to Business Associate's Internal Practices. Except to the extent that it violates or interferes with attorney-client privilege, the duty of client confidentiality, or the applicable rules of professional responsibility, Business Associate will make its internal practices, books, and records, including policies and procedures and PHI, relating to the use and disclosure of (a) PHI received from, or created or received by Business Associate on behalf of, Covered Entity; and (b) EPHI created, received, maintained, or transmitted by Business Associate on behalf of Covered Entity, available to the Secretary or to Covered Entity, in a time and manner designated by the Secretary or reasonably specified by Covered Entity, for purposes of the Secretary determining Covered Entity's compliance with the HIPAA Privacy Regulations and HIPAA Security Regulations.
- 3.11. Breach Notification. Business Associate, following the discovery of a Breach of Unsecured Protected Health Information, shall notify Covered Entity of such breach. Except as otherwise required by law, Business Associate shall provide such notice without unreasonable delay, and in no case later than thirty (30) calendar days after discovery of the Breach.
 - 3.11.1. Notice to Covered Entity required by this Section 3.11 shall include: (i) to the extent possible, the names of the individual(s) whose Unsecured Protected Health Information has been, or is reasonably believed by Business Associate to have been accessed, acquired, used or disclosed during the Breach; (ii) a brief description of what happened including the date of the Breach and the date of the discovery of the Breach, if known; (iii) a description of the types of Unsecured Protected Health Information that were involved in the Breach; (iv) a brief description of what Business Associate is doing or will be doing to investigate the Breach, to mitigate harm to the individual(s), and to protect against further Breaches; and (v) any other information that Covered Entity determines it needs to include in notifications to the individual(s) under 45 C.F.R. § 164.404(c).
 - 3.11.2. After receipt of notice, from any source, of a Breach involving Unsecured Protected Health Information used, disclosed, maintained, or otherwise possessed by Business Associate or of a Breach, involving Unsecured Protected Health Information, for which the Business Associate is otherwise responsible, Covered Entity may in its sole discretion (i) require Business Associate, at Business Associate's sole expense, to use a mutually agreed upon written notice to notify, on Covered Entity's behalf, the

individual(s) affected by the Breach, in accordance with the notification requirements set forth in 45 C.F.R. § 164.404, without unreasonable delay, but in no case later than sixty (60) days after discovery of the Breach; or
(ii) elect to provide notice to the individual(s) affected by the Breach.

- 3.12. Performance of Covered Entity's Obligations. To the extent that Business Associate is to carry out an obligation of Covered Entity under the Privacy Rule, Business Associate shall comply with the requirements of the Privacy Rule that would apply to Covered Entity in the performance of such obligation.

4. Obligations of Covered Entity.

- 4.1. Requested Restrictions. Covered Entity shall notify Business Associate, in writing, of any restriction on the use or disclosure of PHI that Covered Entity has agreed to in accordance with 45 C.F.R. § 164.522, which permits an Individual to request certain restrictions of uses and disclosures, to the extent that such restriction may affect Business Associate's use or disclosure of PHI.
- 4.2. Changes in or Revocation of Permission. Covered Entity will notify Business Associate in writing of any changes in, or revocation of, permission by an Individual to use or disclose PHI, to the extent that such changes or revocation may affect Business Associate's use or disclosure of PHI.
- 4.3. Permissible Requests by Covered Entity. Covered Entity shall not request Business Associate to use or disclose PHI in any manner that would not be permissible under the HIPAA Privacy Regulations and HIPAA Security Regulations if done by Covered Entity, except to the extent that Business Associate will use or disclose PHI for Data Aggregation or management and administrative activities of Business Associate.

5. Security Restrictions on Business Associate.

- 5.1. General. Business Associate shall implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of the EPHI that Business Associate creates, receives, maintains, or transmits on behalf of Covered Entity as required by the HIPAA Security Regulations.
- 5.2. Agents; Subcontractors. Business Associate will ensure that any agent, including a subcontractor, to whom Business Associate provides EPHI agrees to implement reasonable and appropriate safeguards to protect the confidentiality, integrity, and availability of such EPHI.
- 5.3. Reporting of Security Incidents. Business Associate shall report to Covered Entity any Security Incident affecting EPHI created, received, maintained, or transmitted by Business Associate on behalf of Covered Entity, of which Business Associate becomes aware. This Section constitutes notice to Covered Entity of routine and ongoing attempts to gain unauthorized access to Business Associate's information systems (each an "Unsuccessful Attack"), including but not limited to pings, port scans, and denial of service attacks, for which no additional notice shall be required provided that no such incident results in unauthorized access to Electronic PHI.

- 5.4. HIPAA Security Regulations Compliance. Business Associate agrees to comply with Sections 164.308, 164.310, 164.312, and 164.316 of title 45, Code of Federal Regulations.

6. Term and Termination.

- 6.1. Term. This Agreement shall take effect on the start date shown on the first page of the Contract, and shall terminate when all of the PHI provided by Covered Entity to Business Associate, or created or received by Business Associate on behalf of Covered Entity, is destroyed or returned to Covered Entity, or, if it is infeasible to return or destroy PHI, protections are extended to such information, in accordance with the termination provisions in this Section 6.

- 6.2. Termination for Cause. If Covered Entity determines that Business Associate has breached a material term of this Agreement, Covered Entity will provide written notice to Business Associate which sets forth Covered Entity's determination that Business Associate breached a material term of this Agreement, and Covered Entity may:

6.2.1. Provide written notice to Business Associate which provides an opportunity for Business Associate to cure the breach or end the violation, as applicable. If Business Associate does not cure the breach or end the violation within the time specified by Covered Entity, then Covered Entity may immediately thereafter terminate this Agreement; or

6.2.2. Immediately terminate this Agreement if Business Associate has breached a material term of this Agreement and cure is not possible.

6.2.3. If neither termination nor cure is feasible as provided in Sections 6.2.1 and 6.2.2 of this Agreement, Covered Entity will report the violation to the Secretary.

6.3. Effect of Termination.

6.3.1. Except as provided in Section 6.3.2 of this Agreement, upon termination of this Agreement, for any reason, Business Associate will return or destroy all PHI received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity. This provision also applies to PHI that is in the possession of subcontractors or agents of Business Associate. Business Associate will retain no copies of the PHI.

6.3.2. In the event that Business Associate determines that returning or destroying the PHI is infeasible, Business Associate will provide to Covered Entity notification of the conditions that make return or destruction infeasible. Upon reasonable determination that return or destruction of PHI is infeasible, Business Associate will extend the protections of this Agreement to such PHI and limit further uses and disclosures of such PHI to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such PHI.

7. Qualified Service Organization Agreement. Covered Entity and Business Associate hereby acknowledge that Business Associate and its agents and employees have, as applicable, complied, and will comply, with 42 USC §290dd-2 and 42 CFR Ch. 1, part 2, §§2.11 et seq. (the “Federal Drug and Alcohol Regulations”) in that:
 - 7.1. The parties acknowledge that if Business Associate receives, processes, reviews, or otherwise deals with any Covered Entity patient records during the course of the Services Business Associate and its employees will be providing to Covered Entity, that each and every one of said employees will be fully bound by the Federal Drug and Alcohol Regulations;
 - 7.2. Each of Business Associate’s employees and agents will maintain Covered Entity’s patient identifying information in accordance with federal and state confidentiality rules governing drug and alcohol treatment records;
 - 7.3. Each of Business Associate’s employees and agents will comply, as applicable, with the limitations on disclosure, re-disclosure and use set forth in 42 CFR Ch. 1, part 2, §§ 2.16 and 2.53; and
 - 7.4. If necessary, each of Business Associate’s employees and agents will resist in judicial proceedings any efforts to obtain access to patient records except as permitted by the Federal Drug and Alcohol Regulations.
8. Miscellaneous.
 - 8.1. Regulatory References. A reference in this Agreement to a section in the HIPAA Privacy Regulations or the HIPAA Security Regulations means the section as in effect or as amended.
 - 8.2. Amendment. If any new state or federal law, rule, regulation, or policy, or any judicial or administrative decision, affecting the use or disclosure of PHI is enacted or issued, including but not limited to any law or regulation affecting compliance with the requirements of the HIPAA Privacy Regulations or the HIPAA Security Regulations, the parties agree to take such action in a timely manner and as is necessary for Covered Entity and Business Associate to comply with such law, rule, regulation, policy or decision. If the parties are not able to agree on the terms of such an amendment, either party may terminate this Agreement on at least thirty (30) days’ prior written notice to the other party.
 - 8.3. Survival. The respective rights and obligations of Business Associate under Section 6.3 of this Agreement (“Effect of Termination”) shall survive the termination of this Agreement.
 - 8.4. Interpretation. Any ambiguity in this Agreement shall be resolved to permit Covered Entity to comply with the HIPAA Privacy Regulations, the HIPAA Security Regulations, and the Federal Drug and Alcohol Regulations. The section and paragraph headings of this Agreement are for the convenience of the reader only, and are not intended to act as a limitation of the scope or meaning of the sections and paragraphs themselves.
 - 8.5. No Third Party Beneficiaries. Nothing express or implied in this Agreement is

intended to confer, nor shall anything herein confer, upon any person other than Business Associate and Covered Entity and their respective successors or assigns, any rights, remedies, obligations or liabilities whatsoever.

- 8.6. Assignment. This Agreement shall not be assigned or otherwise transferred by either party without the prior written consent of the other, which consent shall not be unreasonably withheld; provided that no such consent shall be required for either party's assignment or transfer of this Agreement in connection with a sale or transfer of all or substantially all of the business or assets of the assigning party. This Agreement shall be binding on and inure to the benefit of the parties hereto and their permitted successors and assigns.
- 8.7. Entire Agreement. This Agreement constitutes the entire agreement between the parties as to its subject matter and supersedes all prior communications, representations, and agreements, oral or written, of the parties with respect to its subject matter.
- 8.8. Severability and Waiver. The invalidity of any term or provision of this Agreement will not affect the validity of any other provision. Waiver by any party of strict performance of any provision of this Agreement will not be a waiver of or prejudice any party's right to require strict performance of the same provision in the future or of any other provision of this Agreement.
- 8.9. Notices. Any notices permitted or required by this Agreement will be addressed as follows or to such other address as either party may provide to the other:

If to Covered Entity: Clark County Department of Community Services
ATTN: County Contact
PO Box 5000
Vancouver, WA 98666-5000

If to Business Associate: Educational Service District
2500 NE 65th Ave
Vancouver, WA 98661

- 8.10. Counterparts. This Agreement may be executed in multiple counterparts, all of which together will constitute one agreement, even though all parties do not sign the same counterpart.

EXHIBIT C**DATA SECURITY REQUIREMENTS**

1. Definitions. The words and phrases listed below, as used in this Exhibit, shall each have the following definitions:
 - a. “AES” means the Advanced Encryption Standard, a specification of Federal Information Processing Standards Publications for the encryption of electronic data issued by the National Institute of Standards and Technology (<http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf>).
 - b. “Authorized Users(s)” means an individual or individuals with a business need to access DSHS Confidential Information, and who has or have been authorized to do so.
 - c. “Category 4 Data” is data that is confidential and requires special handling due to statutes or regulations that require especially strict protection of the data and from which especially serious consequences may arise in the event of any compromise of such data. For purposes of this contract, data classified as Category 4 refers to data protected by: the Health Insurance Portability and Accountability Act (HIPAA).
 - d. “Cloud” means data storage on servers hosted by an entity other than the Contractor and on a network outside the control of the Contractor. Physical storage of data in the cloud typically spans multiple servers and often multiple locations. Cloud storage can be divided between consumer grade storage for personal files and enterprise grade for companies and governmental entities. Examples of consumer grade storage would include iCloud, Dropbox, Box.com, and many other entities. Enterprise cloud vendors include Microsoft Azure, Amazon Web Services, O365, and Rackspace.
 - e. “Encrypt” means to encode Confidential Information into a format that can only be read by those possessing a “key”; a password, digital certificate or other mechanism available only to authorized users. Encryption must use a key length of at least 128 bits (256 preferred and required to be implemented by 06/30/2020) for symmetric keys, or 2048 bits for asymmetric keys. When a symmetric key is used, the Advanced Encryption Standard (AES) must be used if available.
 - f. “Hardened Password” means a string of at least eight characters containing at least three of the following four character classes: Uppercase alphabetic, lowercase alphabetic, numeral, and special characters such as an asterisk, ampersand, or exclamation point.
 - g. “Mobile Device” means a computing device, typically smaller than a notebook, which runs a mobile operating system, such as iOS, Android, or Windows Phone. Mobile Devices include smart phones, most tablets, and other form factors.
 - h. “Multi-factor Authentication” means controlling access to computers and other IT resources by requiring two or more pieces of evidence that the user is who they claim to be. These pieces of evidence consist of something the user knows, such as a password or PIN; something the user has such as a key card, smart card, or physical token; and something the user is, a biometric identifier such as a fingerprint, facial scan, or retinal scan. “PIN” means a personal identification number, a series of numbers which act as a

password for a device. Since PINs are typically only four to six characters, PINs are usually used in conjunction with another factor of authentication, such as a fingerprint.

- i. “Portable Device” means any computing device with a small form factor, designed to be transported from place to place. Portable devices are primarily battery powered devices with base computing resources in the form of a processor, memory, storage, and network access. Examples include, but are not limited to, mobile phones, tablets, and laptops. Mobile Device is a subset of Portable Device.
 - j. “Portable Media” means any machine readable media that may routinely be stored or moved independently of computing devices. Examples include magnetic tapes, optical discs (CDs or DVDs), flash memory (thumb drive) devices, external hard drives, and internal hard drives that have been removed from a computing device.
 - k. “Secure Area” means an area to which only authorized representatives of the entity possessing the Confidential Information have access, and access is controlled through use of a key, card key, combination lock, or comparable mechanism. Secure Areas may include buildings, rooms or locked storage containers (such as a filing cabinet or desk drawer) within a room, as long as access to the Confidential Information is not available to unauthorized personnel. In otherwise Secure Areas, such as an office with restricted access, the Data must be secured in such a way as to prevent access by non-authorized staff such as janitorial or facility security staff, when authorized Contractor staff are not present to ensure that non-authorized staff cannot access it.
 - l. “Trusted Network” means a network operated and maintained by the Contractor, which includes security controls sufficient to protect DSHS Data on that network. Controls would include a firewall between any other networks, access control lists on networking devices such as routers and switches, and other such mechanisms which protect the confidentiality, integrity, and availability of the Data.
 - m. “Unique User ID” means a string of characters that identifies a specific user and which, in conjunction with a password, passphrase or other mechanism, authenticates a user to an information system.
2. Authority. The security requirements described in this document reflect the applicable requirements of Standard 141.10 (<https://ocio.wa.gov/policies>) of the Office of the Chief Information Officer for the state of Washington, and of the DSHS Information Security Policy and Standards Manual. Reference material related to these requirements can be found here: <https://www.dshs.wa.gov/fsa/central-contract-services/keeping-dshs-client-information-private-and-secure>, which is a site developed by the DSHS Information Security Office and hosted by DSHS Central Contracts and Legal Services.
3. Administrative Controls. The Contractor must have the following controls in place:
- a. A documented security policy governing the secure use of its computer network and systems, and which defines sanctions that may be applied to Contractor staff for violating that policy.
 - b. If the Data shared under this agreement is classified as Category 4 data, the Contractor must be aware of and compliant with the applicable legal or regulatory requirements for that Category 4 Data.

- c. If Confidential Information shared under this agreement is classified as Category 4 data, the Contractor must have a documented risk assessment for the system(s) housing the Category 4 Data.

4. Authorization, Authentication, and Access. In order to ensure that access to the Data is limited to authorized staff, the Contractor must:

- a. Have documented policies and procedures governing access to systems with the shared Data.
- b. Restrict access through administrative, physical, and technical controls to authorized staff.
- c. Ensure that user accounts are unique and that any given user account logon ID and password combination is known only to the one employee to whom that account is assigned. For purposes of non-repudiation, it must always be possible to determine which employee performed a given action on a system housing the Data based solely on the logon ID used to perform the action.
- d. Ensure that only authorized users are capable of accessing the Data.
- e. Ensure that an employee's access to the Data is removed immediately:
 - (1) Upon suspected compromise of the user credentials.
 - (2) When their employment, or the contract under which the Data is made available to them, is terminated.
 - (3) When they no longer need access to the Data to fulfill the requirements of the contract.
- f. Have a process to periodically review and verify that only authorized users have access to systems containing DSHS Confidential Information.
- g. When accessing the Data from within the Contractor's network (the Data stays within the Contractor's network at all times), enforce password and logon requirements for users within the Contractor's network, including:
 - (1) A minimum length of 8 characters, and containing at least three of the following character classes: uppercase letters, lowercase letters, numerals, and special characters such as an asterisk, ampersand, or exclamation point.
 - (2) That a password does not contain a user's name, logon ID, or any form of their full name.
 - (3) That a password does not consist of a single dictionary word. A password may be formed as a passphrase, which consists of multiple dictionary words.
 - (4) That passwords are significantly different from the previous four passwords.
- h. When accessing Confidential Information from an external location (the Data will traverse the Internet or otherwise travel outside the Contractor's network), mitigate risk

and enforce password and logon requirements for users by employing measures including:

- (1) Ensuring mitigations applied to the system do not allow end-user modification. Examples would include but not be limited to installing key loggers, malicious software, or any software that will compromise DSHS data.
 - (2) Not allowing the use of dial-up connections.
 - (3) Using industry standard protocols and solutions for remote access. Examples include, but are not limited to RADIUS Microsoft Remote Desktop (RDP) and Citrix.
 - (4) Encrypting all remote access traffic from the external workstation to Trusted Network or to a component within the Trusted Network. The traffic must be encrypted at all times while traversing any network, including the Internet, which is not a Trusted Network.
 - (5) Ensuring that the remote access system prompts for re-authentication or performs automated session termination after no more than 30 minutes of inactivity.
 - (6) Ensuring use of Multi-factor Authentication to connect from the external end point to the internal end point. All Contractors must be in compliance by 06/30/2020.
- i. Passwords or PIN codes may meet a lesser standard if used in conjunction with another authentication mechanism, such as a biometric (fingerprint, face recognition, iris scan) or token (software, hardware, smart card, etc.) in that case:
- (1) The PIN or password must be at least 5 letters or numbers when used in conjunction with at least one other authentication factor
 - (2) Must not be comprised of all the same letter or number (11111, 22222, aaaaa, would not be acceptable)
 - (3) Must not contain a “run” of three or more consecutive numbers (12398, 98743 would not be acceptable)
- j. If the contract specifically allows for the storage of Confidential Information on a Mobile Device, passcodes used on the device must:
- (1) Be a minimum of six alphanumeric characters.
 - (2) Contain at least three unique character classes (upper case, lower case, letter, number).
 - (3) Not contain more than a three consecutive character run. Passcodes consisting of 12345, or abcd12 would not be acceptable.
- k. Render the device unusable after a maximum of 10 failed logon attempts.
5. Protection of Data. The Contractor agrees to store Data on one or more of the following media and protect the Data as described:

- a. Hard disk drives. For Data stored on local workstation hard disks, access to the Data will be restricted to Authorized User(s) by requiring logon to the local workstation using a Unique User ID and Hardened Password or other authentication mechanisms which provide equal or greater security, such as biometrics or smart cards.
- b. Network server disks. For Data stored on hard disks mounted on network servers and made available through shared folders, access to the Data will be restricted to Authorized Users through the use of access control lists which will grant access only after the Authorized User has authenticated to the network using a Unique User ID and Hardened Password or other authentication mechanisms which provide equal or greater security, such as biometrics or smart cards. Data on disks mounted to such servers must be located in an area which is accessible only to authorized personnel, with access controlled through use of a key, card key, combination lock, or comparable mechanism.

For DSHS Confidential Information stored on these disks, deleting unneeded Data is sufficient as long as the disks remain in a Secure Area and otherwise meet the requirements listed in the above paragraph. Destruction of the Data, as outlined below in Section 8 Data Disposition, may be deferred until the disks are retired, replaced, or otherwise taken out of the Secure Area.

- c. Optical discs (CDs or DVDs) in local workstation optical disc drives. Data provided by DSHS on optical discs which will be used in local workstation optical disc drives and which will not be transported out of a Secure Area. When not in use for the contracted purpose, such discs must be Stored in a Secure Area. Workstations which access DSHS Data on optical discs must be located in an area which is accessible only to authorized personnel, with access controlled through use of a key, card key, combination lock, or comparable mechanism.
- d. Optical discs (CDs or DVDs) in drives or jukeboxes attached to servers. Data provided by DSHS on optical discs which will be attached to network servers and which will not be transported out of a Secure Area. Access to Data on these discs will be restricted to Authorized Users through the use of access control lists which will grant access only after the Authorized User has authenticated to the network using a Unique User ID and Hardened Password or other authentication mechanisms which provide equal or greater security, such as biometrics or smart cards. Data on discs attached to such servers must be located in an area which is accessible only to authorized personnel, with access controlled through use of a key, card key, combination lock, or comparable mechanism.
- e. Paper documents. Any paper records must be protected by storing the records in a Secure Area which is only accessible to authorized personnel. When not in use, such records must be stored in a Secure Area.
- f. Remote Access. Access to and use of the Data over the State Governmental Network (SGN) or Secure Access Washington (SAW) will be controlled by DSHS staff who will issue authentication credentials (e.g. a Unique User ID and Hardened Password) to Authorized Users on Contractor's staff. Contractor will notify DSHS staff immediately whenever an Authorized User in possession of such credentials is terminated or otherwise leaves the employ of the Contractor, and whenever an Authorized User's duties change such that the Authorized User no longer requires access to perform work for this Contract.
- g. Data storage on portable devices or media.

- (1) Except where otherwise specified herein, DSHS Data shall not be stored by the Contractor on portable devices or media unless specifically authorized within the terms and conditions of the Contract. If so authorized, the Data shall be given the following protections:
 - (a) Encrypt the Data.
 - (b) Control access to devices with a Unique User ID and Hardened Password or stronger authentication method such as a physical token or biometrics.
 - (c) Manually lock devices whenever they are left unattended and set devices to lock automatically after a period of inactivity, if this feature is available. Maximum period of inactivity is 20 minutes.
 - (d) Apply administrative and physical security controls to Portable Devices and Portable Media by:
 - i. Keeping them in a Secure Area when not in use,
 - ii. Using check-in/check-out procedures when they are shared, and
 - iii. Taking frequent inventories.
 - (2) When being transported outside of a Secure Area, Portable Devices and Portable Media with DSHS Confidential Information must be under the physical control of Contractor staff with authorization to access the Data, even if the Data is encrypted.
- h. Data stored for backup purposes.
- (1) DSHS Confidential Information may be stored on Portable Media as part of a Contractor's existing, documented backup process for business continuity or disaster recovery purposes. Such storage is authorized until such time as that media would be reused during the course of normal backup operations. If backup media is retired while DSHS Confidential Information still exists upon it, such media will be destroyed at that time in accordance with the disposition requirements below in Section 8 Data Disposition.
 - (2) Data may be stored on non-portable media (e.g. Storage Area Network drives, virtual media, etc.) as part of a Contractor's existing, documented backup process for business continuity or disaster recovery purposes. If so, such media will be protected as otherwise described in this exhibit. If this media is retired while DSHS Confidential Information still exists upon it, the data will be destroyed at that time in accordance with the disposition requirements below in Section 8 Data Disposition.
- i. Cloud storage. DSHS Confidential Information requires protections equal to or greater than those specified elsewhere within this exhibit. Cloud storage of Data is problematic as neither DSHS nor the Contractor has control of the environment in which the Data is stored. For this reason:
- (1) DSHS Data will not be stored in any consumer grade Cloud solution, unless all of the following conditions are met:

- (a) Contractor has written procedures in place governing use of the Cloud storage and Contractor attest to the contract listed in the contract and keep a copy of that attestation for your records in writing that all such procedures will be uniformly followed.
 - (b) The Data will be Encrypted while within the Contractor network.
 - (c) The Data will remain Encrypted during transmission to the Cloud.
 - (d) The Data will remain Encrypted at all times while residing within the Cloud storage solution.
 - (e) The Contractor will possess a decryption key for the Data, and the decryption key will be possessed only by the Contractor.
 - (f) The Data will not be downloaded to non-authorized systems, meaning systems that are not on the contractor network.
 - (g) The Data will not be decrypted until downloaded onto a computer within the control of an Authorized User and within the contractor's network.
 - (2) Data will not be stored on an Enterprise Cloud storage solution unless either:
 - (a) The Cloud storage provider is treated as any other Sub-Contractor, and agrees in writing to all of the requirements within this exhibit; or,
 - (b) The Cloud storage solution used is HIPAA compliant.
 - (3) If the Data includes protected health information covered by the Health Insurance Portability and Accountability Act (HIPAA), the Cloud provider must sign a Business Associate Agreement prior to Data being stored in their Cloud solution.
6. System Protection. To prevent compromise of systems which contain DSHS Data or through which that Data passes:
- a. Systems containing DSHS Data must have all security patches or hotfixes applied within 3 months of being made available.
 - b. The Contractor will have a method of ensuring that the requisite patches and hotfixes have been applied within the required timeframes.
 - c. Systems containing DSHS Data shall have an Anti-Malware application, if available, installed.
 - d. Anti-Malware software shall be kept up to date. The product, its anti-virus engine, and any malware database the system uses, will be no more than one update behind current.
7. Data Segregation.
- a. DSHS category 4 data must be segregated or otherwise distinguishable from non-DSHS data. This is to ensure that when no longer needed by the Contractor, all DSHS Data can be identified for return or destruction. It also aids in determining whether DSHS

Data has or may have been compromised in the event of a security breach. As such, one or more of the following methods will be used for data segregation.

- (1) DSHS Data will be kept on media (e.g. hard disk, optical disc, tape, etc.) which will contain no non-DSHS Data.
 - (2) DSHS Data will be stored in a logical container on electronic media, such as a partition or folder dedicated to DSHS Data.
 - (3) DSHS Data will be stored in a database which will contain no non-DSHS data. And/or,
 - (4) DSHS Data will be stored within a database and will be distinguishable from non-DSHS data by the value of a specific field or fields within database records.
 - (5) When stored as physical paper documents, DSHS Data will be physically segregated from non-DSHS data in a drawer, folder, or other container.
- b. When it is not feasible or practical to segregate DSHS Data from non-DSHS data, then both the DSHS Data and the non-DSHS data with which it is commingled must be protected as described in this exhibit.
8. Data Disposition. When the contracted work has been completed or when the DSHS Data is no longer needed, except as noted above in Section 5.b, DSHS Data shall be returned to DSHS or destroyed. Media on which Data may be stored and associated acceptable methods of destruction are as follows:

Data stored on:	Will be destroyed by:
Server or workstation hard disks, or Removable media (e.g. floppies, USB flash drives, portable hard disks) excluding optical discs	Using a “wipe” utility which will overwrite the Data at least three (3) times using either random or single character data, or Degaussing sufficiently to ensure that the Data cannot be reconstructed, or Physically destroying the disk
Paper documents with sensitive or Confidential Information	Recycling through a contracted firm, provided the contract with the recycler assures that the confidentiality of Data will be protected.
Paper documents containing Confidential Information requiring special handling (e.g. protected health information)	On-site shredding, pulping, incineration, or contractor
Optical discs (e.g. CDs or DVDs)	Incineration, shredding, or completely defacing the readable surface with a coarse abrasive
Magnetic tape	Degaussing, incinerating or crosscut shredding

9. Notification of Compromise or Potential Compromise. The compromise or potential compromise of DSHS shared Data must be reported to the DSHS Contact designated in the Contract within one (1) business day of discovery. If no DSHS Contact is designated in the Contract, then the notification must be reported to the DSHS Privacy Officer at dshsprivacyofficer@dshs.wa.gov. Contractor must also take actions to mitigate the risk of loss and comply with any notification or other requirements imposed by law or DSHS.
10. Data shared with Subcontractors. If DSHS Data provided under this Contract is to be shared with a subcontractor, the Contract with the subcontractor must include all of the data security provisions within this Contract and within any amendments, attachments, or exhibits within this Contract. If the Contractor cannot protect the Data as articulated within this Contract, then the contract with the sub-Contractor must be submitted to the DSHS Contact specified for this contract for review and approval.

Certificate Of Completion

Envelope Id: 088A8BA90A3E474E8E063431B8761CA9	Status: Completed
Subject: Please E-Sign This Contract for Developmental Disability Services (ESD 112 Contract #2020-DD-24)	
Source Envelope:	
Document Pages: 32	Signatures: 3
Certificate Pages: 5	Initials: 0
AutoNav: Enabled	Envelope Originator:
Envelopeld Stamping: Enabled	Lynn Mueller
Time Zone: (UTC-08:00) Pacific Time (US & Canada)	1300 Franklin St
	Vancouver, WA 98660
	lynn.mueller@clark.wa.gov
	IP Address: 64.4.181.102

Record Tracking

Status: Original	Holder: Lynn Mueller	Location: DocuSign
7/6/2019 11:25:05 AM	lynn.mueller@clark.wa.gov	

Signer Events

Amanda Migchelbrink
 amanda.migchelbrink@clark.wa.gov
 Deputy Prosecuting Attorney
 Security Level: Email, Account Authentication
 (None)

Signature

DocuSigned by:

 F6B2CB11526542F...
 Signature Adoption: Pre-selected Style
 Using IP Address: 64.4.181.35

Timestamp

Sent: 7/6/2019 11:34:10 AM
 Viewed: 7/8/2019 7:45:34 AM
 Signed: 7/8/2019 7:45:42 AM

Electronic Record and Signature Disclosure:
 Accepted: 7/8/2019 7:45:34 AM
 ID: 5418c0c6-fc2a-4b5a-975d-f9b8d1d32a9b

Tim Merlino
 tim.merlino@esd112.org
 Security Level: Email, Account Authentication
 (None)

DocuSigned by:

 B3237BB86B7C4A8...
 Signature Adoption: Pre-selected Style
 Using IP Address: 107.77.205.236
 Signed using mobile

Sent: 7/8/2019 7:45:43 AM
 Viewed: 7/8/2019 7:57:47 AM
 Signed: 7/8/2019 7:58:04 AM

Electronic Record and Signature Disclosure:
 Accepted: 7/8/2019 7:57:47 AM
 ID: 68a06250-666d-47c9-8271-a9ead8323e66

Lynn Mueller
 lynn.mueller@clark.wa.gov
 Senior Management Analyst
 Clark County Department of Community Services
 Security Level: Email, Account Authentication
 (None)

Completed
 Using IP Address: 64.4.181.102

Sent: 7/8/2019 7:58:05 AM
 Viewed: 7/8/2019 7:58:41 AM
 Signed: 7/11/2019 1:55:08 PM

Electronic Record and Signature Disclosure:
 Not Offered via DocuSign

Tina Redline
 tina.redline@clark.wa.gov
 Office Supervisor
 Clark County, WA
 Security Level: Email, Account Authentication
 (None)

Completed
 Using IP Address: 64.4.181.42

Sent: 7/11/2019 1:55:10 PM
 Viewed: 7/11/2019 2:06:29 PM
 Signed: 7/11/2019 2:06:32 PM

Electronic Record and Signature Disclosure:
 Not Offered via DocuSign

Signer Events	Signature	Timestamp
Shawn Hennessee shawn.hennessee@clark.wa.gov County Manager Clark County, WA Security Level: Email, Account Authentication (None)	 Signature Adoption: Pre-selected Style Using IP Address: 64.4.181.42	Sent: 7/11/2019 2:06:34 PM Viewed: 7/12/2019 9:59:50 AM Signed: 7/12/2019 9:59:53 AM

Electronic Record and Signature Disclosure:
Accepted: 7/31/2018 3:34:36 PM
ID: 23d55715-0ff9-4bb6-9775-6e617676e741

In Person Signer Events	Signature	Timestamp
-------------------------	-----------	-----------

Editor Delivery Events	Status	Timestamp
------------------------	--------	-----------

Agent Delivery Events	Status	Timestamp
-----------------------	--------	-----------

Intermediary Delivery Events	Status	Timestamp
------------------------------	--------	-----------

Certified Delivery Events	Status	Timestamp
---------------------------	--------	-----------

Carbon Copy Events	Status	Timestamp
--------------------	--------	-----------

Janet Snook janet.snook@clark.wa.gov testing dcs Security Level: Email, Account Authentication (None)		Sent: 7/12/2019 9:59:54 AM Viewed: 7/12/2019 11:28:21 AM
---	---	---

Electronic Record and Signature Disclosure:
Not Offered via DocuSign

Witness Events	Signature	Timestamp
----------------	-----------	-----------

Notary Events	Signature	Timestamp
---------------	-----------	-----------

Envelope Summary Events	Status	Timestamps
-------------------------	--------	------------

Envelope Sent	Hashed/Encrypted	7/12/2019 9:59:54 AM
Certified Delivered	Security Checked	7/12/2019 9:59:54 AM
Signing Complete	Security Checked	7/12/2019 9:59:54 AM
Completed	Security Checked	7/12/2019 9:59:54 AM

Payment Events	Status	Timestamps
----------------	--------	------------

Electronic Record and Signature Disclosure
--

CONSUMER DISCLOSURE

From time to time, Clark County, WA (we, us or Company) may be required by law to provide to you certain written notices or disclosures. Described below are the terms and conditions for providing to you such notices and disclosures electronically through the DocuSign, Inc. (DocuSign) electronic signing system. Please read the information below carefully and thoroughly, and if you can access this information electronically to your satisfaction and agree to these terms and conditions, please confirm your agreement by clicking the "I agree"™ button at the bottom of this document.

Getting paper copies

At any time, you may request from us a paper copy of any record provided or made available electronically to you by us. You will have the ability to download and print documents we send to you through the DocuSign system during and immediately after signing session and, if you elect to create a DocuSign signer account, you may access them for a limited period of time (usually 30 days) after such documents are first sent to you. After such time, if you wish for us to send you paper copies of any such documents from our office to you, you will be charged a \$0.00 per-page fee. You may request delivery of such paper copies from us by following the procedure described below.

Withdrawing your consent

If you decide to receive notices and disclosures from us electronically, you may at any time change your mind and tell us that thereafter you want to receive required notices and disclosures only in paper format. How you must inform us of your decision to receive future notices and disclosure in paper format and withdraw your consent to receive notices and disclosures electronically is described below.

Consequences of changing your mind

If you elect to receive required notices and disclosures only in paper format, it will slow the speed at which we can complete certain steps in transactions with you and delivering services to you because we will need first to send the required notices or disclosures to you in paper format, and then wait until we receive back from you your acknowledgment of your receipt of such paper notices or disclosures. To indicate to us that you are changing your mind, you must withdraw your consent using the DocuSign "Withdraw Consent"™ form on the signing page of a DocuSign envelope instead of signing it. This will indicate to us that you have withdrawn your consent to receive required notices and disclosures electronically from us and you will no longer be able to use the DocuSign system to receive required notices and consents electronically from us or to sign electronically documents from us.

All notices and disclosures will be sent to you electronically

Unless you tell us otherwise in accordance with the procedures described herein, we will provide electronically to you through the DocuSign system all required notices, disclosures, authorizations, acknowledgements, and other documents that are required to be provided or made available to you during the course of our relationship with you. To reduce the chance of you inadvertently not receiving any notice or disclosure, we prefer to provide all of the required notices and disclosures to you by the same method and to the same address that you have given us. Thus, you can receive all the disclosures and notices electronically or in paper format through the paper mail delivery system. If you do not agree with this process, please let us know as described below. Please also see the paragraph immediately above that describes the consequences of your electing not to receive delivery of the notices and disclosures

electronically from us.

How to contact Clark County, WA:

You may contact us to let us know of your changes as to how we may contact you electronically, to request paper copies of certain information from us, and to withdraw your prior consent to receive notices and disclosures electronically as follows:

To contact us by email send messages to: loann.vuu@clark.wa.gov

To advise Clark County, WA of your new e-mail address

To let us know of a change in your e-mail address where we should send notices and disclosures electronically to you, you must send an email message to us at loann.vuu@clark.wa.gov and in the body of such request you must state: your previous e-mail address, your new e-mail address. We do not require any other information from you to change your email address..

In addition, you must notify DocuSign, Inc. to arrange for your new email address to be reflected in your DocuSign account by following the process for changing e-mail in the DocuSign system.

To request paper copies from Clark County, WA

To request delivery from us of paper copies of the notices and disclosures previously provided by us to you electronically, you must send us an e-mail to loann.vuu@clark.wa.gov and in the body of such request you must state your e-mail address, full name, US Postal address, and telephone number. We will bill you for any fees at that time, if any.

To withdraw your consent with Clark County, WA

To inform us that you no longer want to receive future notices and disclosures in electronic format you may:

- i. decline to sign a document from within your DocuSign session, and on the subsequent page, select the check-box indicating you wish to withdraw your consent, or you may;
- ii. send us an e-mail to loann.vuu@clark.wa.gov and in the body of such request you must state your e-mail, full name, US Postal Address, and telephone number. We do not need any other information from you to withdraw consent.. The consequences of your withdrawing consent for online documents will be that transactions may take a longer time to process..

Required hardware and software

Operating Systems:	Windows® 2000, Windows® XP, Windows Vista®; Mac OS® X
Browsers:	Final release versions of Internet Explorer® 6.0 or above (Windows only); Mozilla Firefox 2.0 or above (Windows and Mac); Safari®, 3.0 or above (Mac only)
PDF Reader:	Acrobat® or similar software may be required to view and print PDF files
Screen Resolution:	800 x 600 minimum
Enabled Security Settings:	Allow per session cookies

** These minimum requirements are subject to change. If these requirements change, you will be asked to re-accept the disclosure. Pre-release (e.g. beta) versions of operating systems and browsers are not supported.

Acknowledging your access and consent to receive materials electronically

To confirm to us that you can access this information electronically, which will be similar to other electronic notices and disclosures that we will provide to you, please verify that you were able to read this electronic disclosure and that you also were able to print on paper or electronically save this page for your future reference and access or that you were able to e-mail this disclosure and consent to an address where you will be able to print on paper or save it for your future reference and access. Further, if you consent to receiving notices and disclosures exclusively in electronic format on the terms and conditions described above, please let us know by clicking the "I agree"™ button below.

By checking the "I agree"™ box, I confirm that:

- I can access and read this Electronic CONSENT TO ELECTRONIC RECEIPT OF ELECTRONIC CONSUMER DISCLOSURES document; and
- I can print on paper the disclosure or save or send the disclosure to a place where I can print it, for future reference and access; and
- Until or unless I notify Clark County, WA as described above, I consent to receive from exclusively through electronic means all notices, disclosures, authorizations, acknowledgements, and other documents that are required to be provided or made available to me by Clark County, WA during the course of my relationship with you.